GSA

E-Authentication Implementation Workshop

Developing a Project Plan

April 12 & 14, 2005

E·GOV

Project Plan: Outline

- Planning & Analysis
- Design & Development
- Acceptance Testing
- Boarding Process

Planning & Analysis: Boarding Process

- Process by which application owners “board” the E-Authentication Federation
- Identifies steps necessary to successfully complete the process, including:
  - Execute various agreements
  - Declare compliance with several government-wide policies
  - Meet E-Authentication architecture/technical interface requirements

Planning & Analysis: Business Considerations

- Determine Application Assurance Level
- Discuss Potential End User Credential Providers
- Discuss/Develop Linking Strategy
- Consider Communications and Outreach Requirements
- Plan for Legal Review

Planning & Analysis: Technical Requirements

- Perform System Requirements Analysis
- Develop End User Requirements
- Determine Network Security Requirements
- Develop Risk Assessment/Management Plan
- Identify Appropriate Level CSs

Planning & Analysis: Landing Page Requirements

- What is a landing page?
- Do you plan to support this, yes or no?
- Assess Impacts
  - User Experience
  - User Interface
  - System Requirements
- Customer Service Perspectives

Planning & Analysis: Operational Requirements

- Determine Help Desk Requirements
- Develop Transaction & Audit Logging Requirements
- Perform Business Continuity Impact
- Create Network Security Rules to Enable Connectivity
- Update C&A Plan, FISMA Requirements

Planning & Analysis: Milestones

- OMB-Defined Assurance Level Determined
- System Requirements Specification
  - Expected to be Part of Application Development Process
  - Deliverable to E-Authentication
  - Addresses the Requirements of the System/Application
    - Functional Requirements
    - Interface Requirements
    - Data Requirements
  - Allows E-Authentication to Better Support Integration with E-Auth Components

Design and Develop

- Build Detailed Project Plan
- Develop Detailed Functional Requirements
- Create Systems Design Document

Design & Develop: Milestones

- Updated Project Plan
- System Design Document
  - Expected to be Part of Application Development Process
  - Deliverable to E-Authentication
  - Addresses the Requirements of the System/Application
    - Details the Architectural Design of the System/Application to Meet the System Requirements
    - Details the Interface of Components External to the System/Application
    - Details the Data Utilized by the System/Application, both Internal and External to the System/Application
  - Allows E-Authentication to Better Support Integration with E-Auth Components

Design & Develop

- Schedule Acceptance Testing
  - 2-3 months in advance
  - Must be prepared for testing or risk re-schedule
- Identify SAML/PKI Product Requirements
- Evaluate SAML/PKI Products
- Develop Functional Test Strategy
- Determine Applicable E-Auth Use Cases

Design & Develop: Hint List Strategy (PKI)

- "Hint List" is not a "Trust List"
- Used to Assist End-User in Selecting an Appropriate Certificate Assuming the End-User has More than One
- Web servers requiring client certificates for user authentication must provide to the user's browser (during the SSL/TLS tunnel setup phase) a list of all CAs from which the web server is willing to accept end-user certificates: *The Hint List*
- The user's browser presents to the user a pick list of all client certificates that have been issued by a CA on the Hint List or a subordinate CA
- The web server must know *before the transaction is attempted* all possible issuing CAs

Design & Develop: Activation

- Determine Activation Approach
- What is Activation?
- How does an AA map the information in an identity assertion (SAML or PKI cert) to an entry in the AA's database of users?

Design & Develop: Assertion Contents

- Current SAML Assertion Attributes:
  - Credential Service ID (CSid)
  - Unique User ID (Uid)
  - Name
  - Assurance Level of CS
- Proposed Optional Assertion Attributes:
  - First, Middle, Last Names, Generation Qualifier
  - Partial SSN
  - DOB
  - Address
  - Session ID (Sid)

Design & Develop: Types of Activation

- Automatic
- Prompted
- Deferred
- None

Design & Develop: Automatic Activation

- Mapping occurs solely from content of identity assertion
- AA has own database of users
- Extensible to include:
  - SAML: CSid and Uid
  - PKI: issuer and serial number
- Accuracy of database contents
- Attainable high percentage of time

Design & Develop: Prompted Activation

- Mapping with contents of identity assertion and additional information from end user when prompted by AA
- AA has own database of users
- Extensible to include:
  - SAML: CSid and Uid
  - PKI: issuer and serial number
- Accuracy of database contents
- Attainable high percentage of time
- Might use knowledge-based service

Design & Develop: Deferred Activation

- Uses out-of-band process
- Usually not real-time
- AA has own database of users
- Extensible to include:
  - SAML: CSid and Uid
  - PKI: issuer and serial number
- No suitable mapping policies/techniques
- Limited access may be available

Design & Develop: No Activation

- Information in identity assertion unknown to AA
- Perhaps no database of users
- Treated as new user registration

Design & Develop: Activation Considerations

- Strategy Selection
- Supporting Multiple Credentials
  - Support 2+ Credentials
  - Overwrite
  - Create new user
- Activation Failure
  - Hybrid approach
  - Landing page
- Other Considerations
  - Deactivation
  - Reactivation

Design & Develop

- Develop Exception Handling Approach
- Develop Redirection of Unauthenticated Users
- Develop Landing Page

Design & Develop: User Interface Design

- Verify Section 508 Compliance
- Perform Usability Analysis
- Integrate E-Auth Branding

Design & Develop: Usability

- New UI for E-Authentication Portal
- “Expert” & “Novice” modes
- User type (a la FirstGov)
- Recommendations to AAs and CSs to improve continuity
- Exception handling

Design & Develop

- Code Development
  - Implement Requirements
  - SAML: Implement SAML Interface Specification
  - PKI: Implement Certificate Validation Approach
- Implement Federation Time Synch

Design & Develop: Sandbox Testing (SAML)

- Implementation Assistance
- Transfer lessons learned/minimize wheel reinvention
- Preparation for full acceptance testing
- Flavors
  - SAML Catch
  - Sandbox Testing
- E-GCA Certificates
  - SSL Certificates Required for Exchanged Data Between E-Auth Components
  - AA Must Request EGCA Test Certificates from E-Auth via Relationship Manager

Acceptance Testing—SAML

- Ensures that the Implemented SAML Product has been Installed and Configured Correctly
- Must Be Scheduled with Lab In Advance
  - Expect 3 days to 2 weeks (depending on level of preparation)
- Validate AA Is Ready for Acceptance Testing
  - Error Handling
  - EGCA Certificates
  - Configured for SAML 1.0 Browser-Artifact Profile
  - Metadata Implemented
  - Open Application Server Ports
- **Milestone**
  - Lab Pre-Requisites Checklist Completed

Acceptance Testing—SAML

- Confirm Systems Are Tested in Production-Ready Environment
- Test Use Cases
- Test Compliance to Interface Spec
- **Milestone**
  - Successful Acceptance Testing

Certificate Validation Testing—PKI

- Ensures that the Implemented Certificate Validation Product Interoperates with Federal PKI
- Must Be Scheduled with Lab In Advance
  - 2-3 months
  - Must Be Prepared Or Risk Rescheduling
- Certificate Validation Testing
  - Test Validation Using Certificates Issued by the Set (or a Subset) of Cross-Certified CAs

Boarding Checklist

Requirements:	Yes	No	N/A	Evidence
Signatures: *Every member that joins the E-Authentication Federation must sign agreements with the E-Authentication Program Office.*				
Memorandum of Understanding or Contract				Signed Document
Participation Agreement				Signed Document (Business Rules)
Service Level Agreement				Signed Document (Operating Rules)
Completed Privacy Impact Assessment (government only)				url
Declarations: *Some required documents are sensitive so are inappropriate to provide as evidence, or they are publicly accessible documents and are therefore unnecessary to reproduce as evidence. Declaration of a document's completeness satisfies the documentation requirement.*				
Completed System of Records Notice (government only)				
Authority to Operate (ATO) updated for E-Authentication Architecture				
Usability/Section 508 Compliance (government only)				
Paperwork Reduction Act (PRA) Compliance (government only)				OMB PRA#

Boarding Checklist (Cont'd)

Critical Tasks *The following tasks must be completed before a participant can join the E-Authentication Federation:*				
If an Agency Application: Completed e-RA or similar documentation				Copy of e-RA
If a Credential Service: Completed Credential Assessment				Copy of Credential Assessment and Approval Letter
Acceptance Test Completed in Interoperability Lab				Copy of Acceptance Test Report
Boarding Approval				Evaluator Approval on Checklist

Boarding Process

- Validate Boarding Checklist is Completed
- Request and Install Production EGCA Certificate
- Install production metadata
- Test in staging environment
- If CSP, addition to Trust List
- Activate Application/CSP on E-Authentication Portal

Boarding Milestones

- Completed Boarding Checklist
- Completed Boarding Process
- Live E-Authentication-Enabled Application!